CAICT 中国信通院

筑牢下一代互联网安全防线

—IPv6 网络安全白皮书

中国信息通信研究院

2019年9月

版权声明

前　言

当前，网络信息技术加速引领新一轮科技革命，以前所未有的广度和深度引发经济社会多方位、全领域、深层次的技术创新和产业变革。在5G、物联网、工业互联网等新兴领域蓬勃发展，人人互联加速向万物互联迈进的时代趋势下，网络空间传统 IPv4 地址资源紧缺等问题日益凸显，以 IPv6 为代表的下一代互联网技术应运而生。IPv6 凭借其海量地址空间、内嵌安全能力等技术优势，为泛在融合、大连接的新形势下网络信息技术的创新发展提供基础网络资源支撑，已成为促进生产生活数字化、网络化、智能化发展的核心要素，吸引世界发达国家的广泛关注和大力投入。

近年来，我国紧抓全球网络信息技术加速创新变革、信息基础设施快速演进升级的历史机遇，全力推进下一代互联网部署应用，为经济社会发展和网络强国建设提供有力支撑。然而，IPv4 向 IPv6 网络的升级演进是一个长期、持续的过程，现阶段已部署上线的 IPv6 业务仍相对有限，IPv6 部署应用过程中的网络安全风险尚未完全显现。此种客观情况对IPv6 新环境下的网络安全防御工作而言是挑战也是机遇，与传统网络安全防御攻击方更为被动的形势相比，在 IPv6 环境中，攻防双方正处于同一起跑线上。我们更应高度重视下一代互联网演进升级中存在的安全风险，加快提升 IPv6 网络安

全防护能力，构建形成 IPv6 网络安全防护主动局面。

我院联合安天科技股份有限公司、北京蓝汛通信技术有限责任公司、北京天融信网络安全技术有限公司、北京知道创宇信息技术股份有限公司、北京神州绿盟信息安全科技股份有限公司、华为技术有限公司、杭州安恒信息技术股份有限公司、奇安信科技集团股份有限公司、上海观安信息技术股份有限公司、深信服科技股份有限公司、深圳市腾讯计算机系统有限公司、网宿科技股份有限公司、亚信科技（成都）有限公司、中国电信集团有限公司、中国联合网络通信集团有限公司、中国移动通信集团有限公司[1]共同推出《筑牢下一代互联网安全防线—IPv6 网络安全白皮书》。本白皮书从网络安全视角，客观审视 IPv6 发展和网络安全工作现状，分析探讨下一代互联网升级演进过程中的安全风险和应对举措，梳理现有网络安全工作急需，挖掘 IPv6 安全产品和服务重点发展方向，希望与业界分享，共同推动保障下一代互联网安全、有序发展。

[1] 注：按首字母排序，排名不分先后

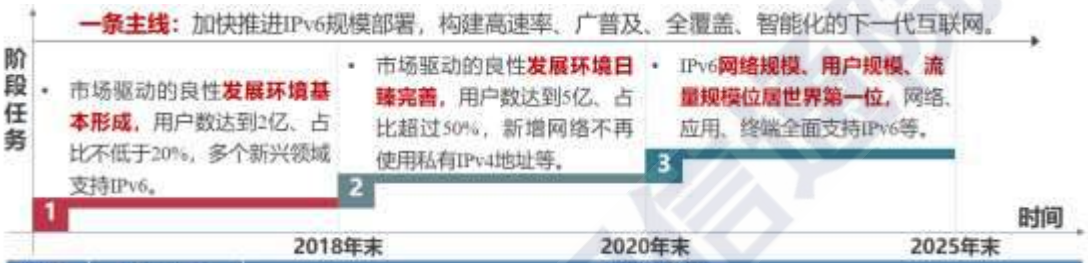
目 录

一、相关背景 1
（一）IPv6 改造稳步推进，基本形成市场驱动良性环境 1
1、网络基础设施 IPv6 升级改造基本完成 1
2、应用基础设施已具备 IPv6 服务能力 3
3、互联网应用 IPv6 活跃用户数稳步提升 4
（二）IPv6 安全风险开始显现，挑战下一代互联网安全保障能力 . 5
1、IPv6 网络攻击数量剧增，攻击范围逐渐扩大 6
2、IPv6 安全漏洞客观存在，影响覆盖系统、应用等各相关层面 . . 7
二、我国下一代互联网建设安全工作现状 8
（一）贯彻落实国家战略，加强 IPv6 安全工作部署 8
1、工信部：明确 IPv6 安全工作阶段性目标 9
2、广电总局：细化 IPv6 安全指导和安全测试验证要求 9
3、教育部：强调 IPv6 安全保障体系总体目标 10
4、央行：同步落实 IPv6 发展和安全工作 11
（二）加快 IPv6 安全科研布局，强化 IPv6 安全技术储备 11
1、强化 IPv6 安全核心要素和基础资源安全管理创新 12
2、开展 IPv6 安全风险研究，构建 IPv6 安全应对体系 13
3、推动 IPv6 源地址认证和网络攻击追踪溯源研究 14
（三）推动 IPv6 安全实践，强化 IPv6 安全创新 16
1、加快 IPv6 安全标准制修订，强化 IPv6 安全指导 16
2、加强 IPv6 安全产品和服务探索，助力安全能力提升 17

3、探索 IPv6 安全解决方案，强化 IPv6 安全风险应对 18
三、我国下一代互联网建设仍面临的安全挑战 20
（一）IPv4/IPv6 长期并存，过渡机制持续叠加安全风险 20
1、双栈机制：IPv4/IPv6 网络安全暴露面倍增 21
2、隧道机制：内置安全功能缺失，安全影响范围扩大 22
3、翻译机制：机制内在特性仍面临传统网络攻击威胁 23
（二）协议新特性挑战现有安全手段，融合场景风险持续扩大 .. 25
1、IPv6 地址标识复杂性骤增，挑战基于地址资源安全防护手段 . 25
2、IPv6 协议新特性引入新安全问题，网络安全风险此消彼长 ... 27
3、IPv6 融合场景放大新技术安全隐患，加剧安全防御被动局面 . 30
（三）IPv6 网络安全需求能力“剪刀差”亟需弥合 31
1、IPv6 安全产品发展尚在起步，远滞后安全能力需求 31
2、IPv6 安全问题未充分暴露，制约安全服务发展步伐 33
3、“IPv6+网络安全”复合型专业技术人才缺失 34
四、保障下一代互联网安全有序发展的建议 34
（一）主动布局 IPv6 安全产品服务和安全实践推广 35
（二）按需求、分场景落实 IPv6 安全产品服务部署 39
（三）构建 IPv6 安全创新机制，强化 IPv6 风险防范能力建设 .. 43
（四）强化 IPv6 安全知识技能培训，弥合 IPv6 安全人才差距 .. 44

一、相关背景

近年来，我国紧抓全球信息通信技术加速创新变革、信息基础设施快速演进升级的历史机遇，在国家层面出台《推进互联网协议第六版（IPv6）规模部署行动计划》（以下简称《行动计划》），提出**“一条主线、三个阶段、五项任务”总体目标，**全力推进互联网演进升级和健康创新发展，如图 1.1 所示。



编号	重点任务	任务要求
1	互联网应用	升级典型应用/升级政府、中央媒体、中央企业网站/创新特色应用
2	网络基础设施	升级改造移动和固定网络/推广移动和固定终端应用/实现骨干网互联互通/扩容国际出入口等
3	应用基础设施	升级改造互联网数据中心/升级改造内容分发网络和云服务平台/升级改造域名系统等
4	网络安全能力	升级安全系统/强化地址管理/加强安全防护/构筑新兴领域安全保障能力
5	前沿技术创新	加强IPv6关键技术研发/强化网络前沿技术创新

图 1.1 我国下一代互联网建设总体目标

目前，我国下一代互联网建设第一阶段目标任务全面完成，网络设施全面就绪、应用改造逐步推进、活跃用户稳步提升的局面已经形成。但随着下一代互联网网络和业务环境逐步成熟，IPv6 网络安全风险开始逐渐浮出水面，IPv6 网络安全事件时有发生。

（一）IPv6 改造稳步推进，基本形成市场驱动良性环境

1、网络基础设施 IPv6 升级改造基本完成

目前，我国固网、LTE 网络已大规模分配 IPv6 地址，基本具备 IPv6 业务承载能力[2]。截止 2019 年 7 月，LTE **网络方面，**全国 30 省[3]

[2] 数据来源：本节数据如无特别说明，均统计自推进 IPv6 规模部署专家委员会。
[3] 数据统计范围不包括香港、澳门、台湾、新疆。

的 LTE 网络已完成 IPv6 升级改造；**固定网络方面，**基础电信企业骨干网设备已全部支持 IPv6，13 个骨干网直联点已全部实现 IPv6 互联互通，全国 30 个省城域网 IPv6 改造已经全面完成；**国际出入口方面，**基础电信企业已开通 IPv6 国际出入口带宽 100Gbps，扩建工作不断加快。IPv6 网络流量现状如图 1.2 所示。

图 1.2 IPv6 流量现状

随着网络基础设施 IPv6 升级改造工作的持续推进，IPv6 网络相关用户数稳步增长。截止 2019 年 7 月，全国已有 12.78 亿用户获得 IPv6 地址，其中，LTE 网络用户共 11.29 亿，固定网络用户 1.49 亿，相比 2018 年初增长超过 10 倍，如图 1.3 所示。

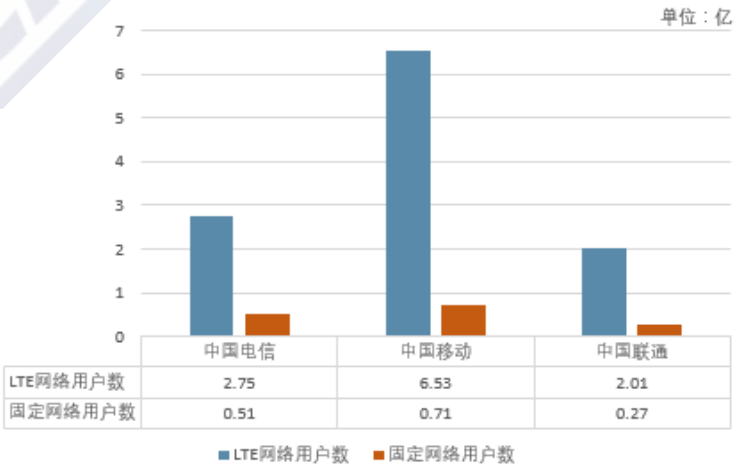
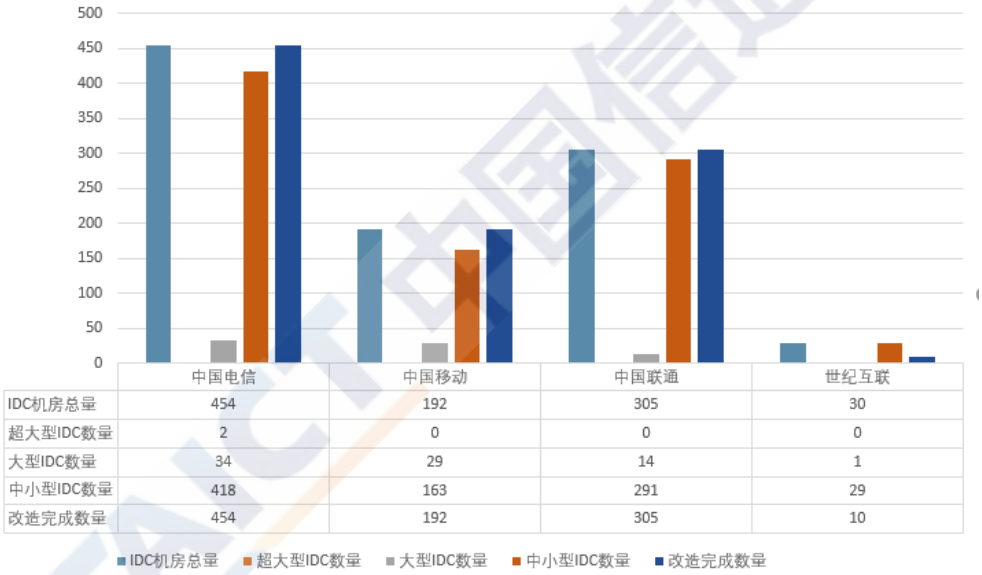


图 1.3 IPv6 用户数现状

2、应用基础设施已具备 IPv6 服务能力

我国应用基础设施改造速度不断加快，已具备全国范围内对外提供服务的能力。DNS **方面，**我国国家顶级域名服务系统早在 2012 年的 CNGI[4]二期工程中已完成 IPv6 升级改造。截止 2019 年 7 月，基础电信企业递归域名服务器已全部完成 IPv6 升级改造，全面支持 IPv6 地址解析。IDC **方面，**基础电信企业超大型/大型/中小型 IDC[5]升级改造全面完成，世纪互联等企业已完成大型 IDC 升级改造，正加快推动中小型 IDC 升级改造进度，如图 1.4 所示。



	中国电信	中国移动	中国联通	世纪互联
IDC机房总量	454	192	305	30
超大型IDC数量	2	0	0	0
大型IDC数量	34	29	14	1
中小型IDC数量	418	163	291	29
改造完成数量	454	192	305	10

图 1.4 IDC 升级改造现状

CDN **方面，**我国 CDN 企业全部机房 IPv6 覆盖能力已达 100%，已具备面向全国提供 IPv6 相关业务加速能力，省级 CDN 节点本地部署已超过 60%，如图 1.5 所示。

[4] CNGI：China's Next Generation Internet，中国下一代互联网。
[5] 以功率为 2.5 千瓦的标准机架为换算单位，超大型数据中心是指规模大于等于 10000 个标准机架的数据中心；大型数据中心是指规模大于等于 3000 个标准机架小于 10000 个标准机架的数据中心；中小型数据中心是指规模小于 3000 个标准机架的数据中心。

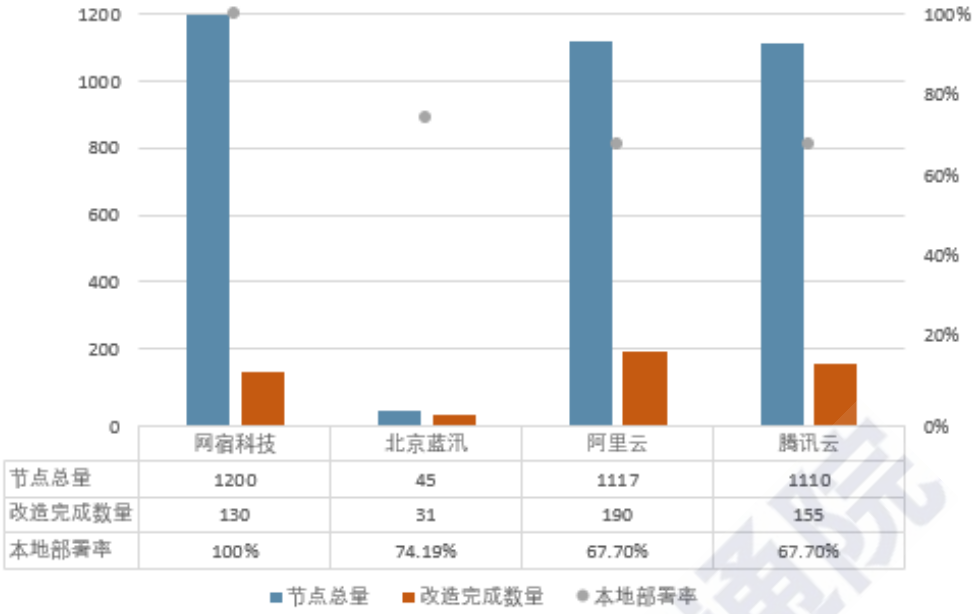


图 1.5 CDN 升级改造现状

云平台方面，阿里云、百度云、腾讯云等知名云服务平台持续推进云服务产品 IPv6 升级改造。目前，负载均衡、对象存储、域名解析等不同种类云服务产品已完成 IPv6 升级改造，平均改造率已超过 60%，如图 1.6 所示。

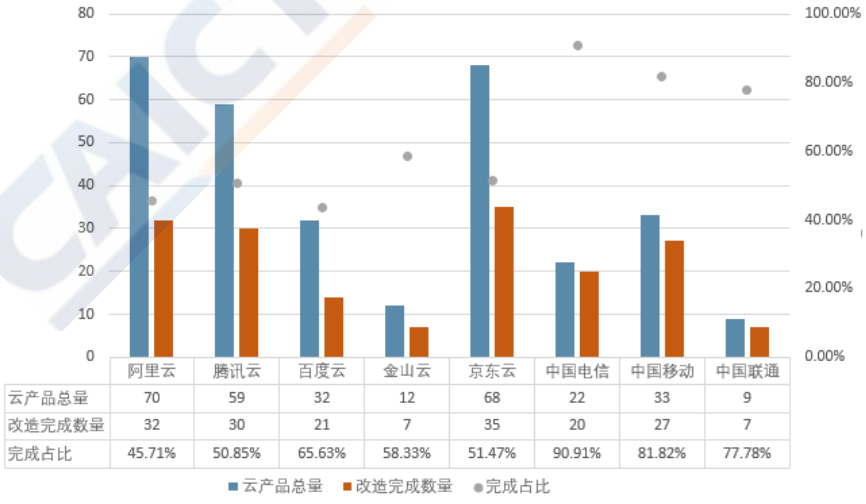


图 1.6 云平台升级改造现状

3、互联网应用 IPv6 活跃用户数稳步提升

随着网络及应用基础设施 IPv6 升级改造的持续推进，IPv6 网络和应用能力稳步提升，IPv6 相关业务开始逐步上线，购物、视频、新

闻等各类互联网应用 IPv6 活跃用户数稳步提升。截止 2019 年 7 月，我国主要互联网应用活跃用户数已达 2.01 亿，如图 1.7 所示。

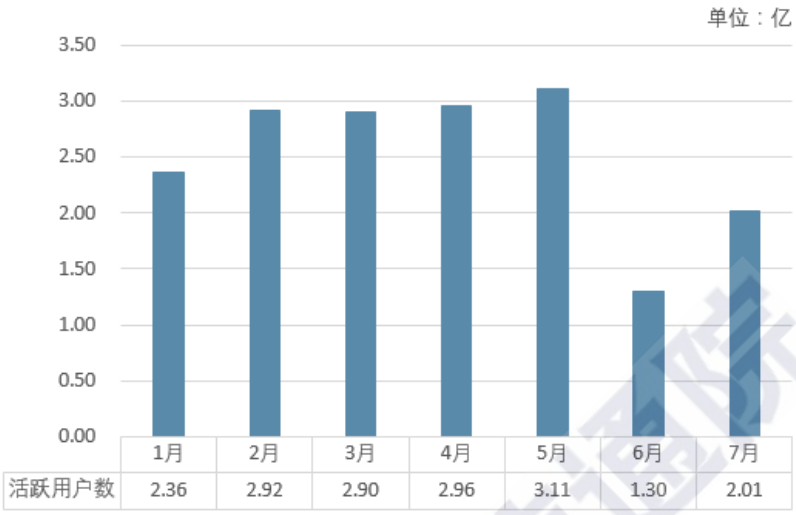


图 1.7 2019 年我国 IPv6 活跃用户数增长情况

此外，截止 2019 年 7 月，我国政府、央企、央媒、商业[6]等各类网站 IPv6 升级改造也已取得积极进展，如图 1.8 所示。

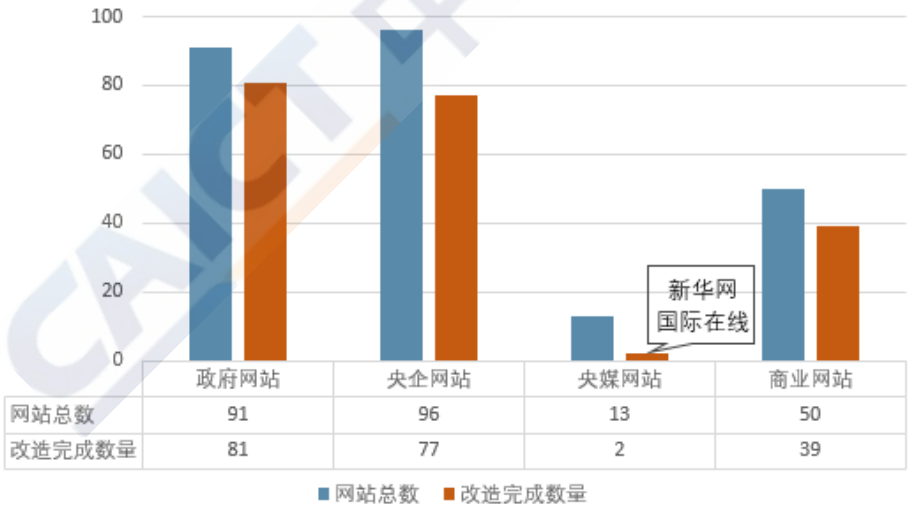


图 1.8 各类网站升级改造现状

（二）IPv6 安全风险开始显现，挑战下一代互联网安全保障能力

早在 2018 年 3 月，美国安全厂商 Neustar 已发现业内第一起基

[6] 统计维度为排名前 50 的商业网站。

于 IPv6 协议的 DDoS 攻击，攻击对象为存储 1900 个 IPv6 地址的 DNS 服务器[7]。近年来，随着我国 IPv6 网络和业务开始上线，IPv6 网络攻击事件也开始出现，IPv6 网络安全问题相继浮出水面，我国下一代互联网建设正面临客观安全挑战。

1、IPv6 网络攻击数量剧增，攻击范围逐渐扩大

随着 IPv6 网络开始投入使用，IPv6 网络攻击[8]数量急剧增加，影响范围也呈现出向各行业领域扩大趋势。据国内安全厂商统计，2019 年上半年共监测发现超过 9 万起 IPv6 网络攻击，其中，攻击对象覆盖政府部门、事业单位、教育机构等单位[9]，如图 1.9 所示。

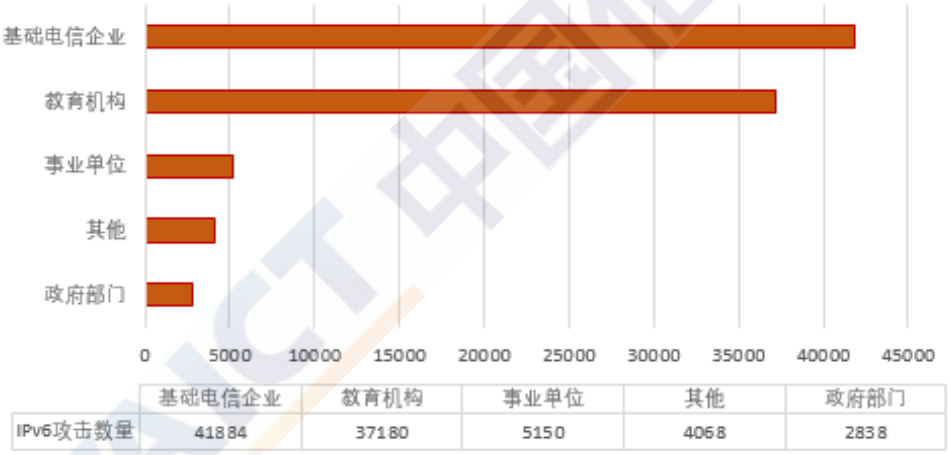


图 1.9 2019 年上半年政企事业单位遭受 IPv6 攻击情况

在 2019 年 3 月，国内安全厂商拦截到攻击源为 IPv6 地址的网络攻击 8000 万起[10]；在针对 283 家政府部门、教育机构、中央企业云托管网站来自 IPv6 网络的攻击中，目录遍历攻击、WEB Shell 攻击、SQL 注入等典型 WEB 攻击超过 90%[11]，如图 1.10 所示。

[7] IPv6 环境下需要 DNS 存储海量地址，导致 DNS 极易被攻击者选为攻击的关键对象。
[8] IPv6 网络攻击包括攻击源为 IPv6 地址的攻击，以及利用 IPv6 网络或安全问题发起的各类攻击。
[9] 数据来源：据神州绿盟整理统计。
[10] 数据来源：据知道创宇整理统计。
[11] 数据来源：据深信服整理统计。

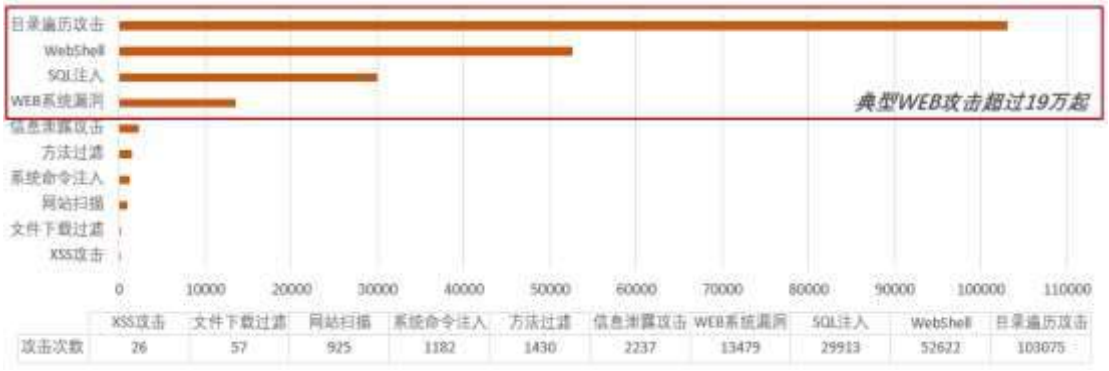


图 1.10 283 家云托管网站网络攻击情况

2、IPv6 安全漏洞客观存在，影响覆盖系统、应用等各相关层面

尽管 IPv6 相关技术概念早在 1996 年已经提出，但直到近年来才开始引起各界的广泛关注和投入，相关硬件终端、操作系统、软件应用等仍处部署应用初期阶段，尚不具备较为完善的安全机制，IPv6 安全漏洞客观存在。截止 2019 年 7 月，CVE 漏洞库中已收录 IPv6 相关漏洞 381 条，覆盖系统漏洞、应用漏洞、硬件漏洞、协议漏洞等不同层面，如图 1.11 所示。

图 1.11 IPv6 相关漏洞情况（保留四舍五入统计误差）

其中，CVSS[12]评分超过 7 的高危漏洞占比超过 50%，如图 1.12 所示。

[12] CVSS：Common Vulnerability Scoring System，通用漏洞评分系统。

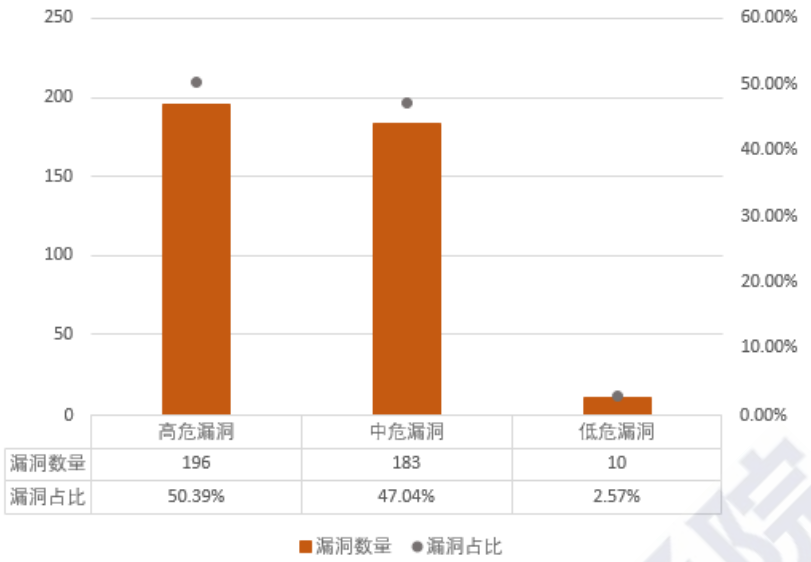


图 1.12 不同威胁程度漏洞分布情况

二、我国下一代互联网建设安全工作现状

自《行动计划》发布以来，我国政产学研各界贯彻落实国家重大战略要求，从工作部署、科研工作、产品服务、安全实践等方面全面强化下一代互联网安全布局，持续加强我国下一代互联网安全保障。

（一）贯彻落实国家战略，加强 IPv6 安全工作部署

近年来，我国各政府部门立足自身职责分工，在政策方面频频发力，出台部门相关政策文件，同步强化各行业领域 IPv6 发展和安全工作部署，如图 2.1 所示。

政府部门	职责分工	发布时间	政策文件
工信部	网络基础设施 应用基础设施 基础电信企业网站等	2018年5月2日	《关于贯彻落实<推进互联网协议第六版（IPv6）规模部署行动计划>的通知》
		2019年4月16日	《关于开展2019年IPv6网络就绪专项行动的通知》
国资委	中央企业网站	2018年3月12日	《关于做好互联网协议第六版（IPv6）部署应用有关工作的通知》
广电总局	中央媒体网站	2019年2月3日	《广电有线网络IPv6规模部署及推进实施指南》
教育部	教育系统网站	2018年8月21日	《教育部办公厅关于贯彻落实<推进互联网协议第六版（IPv6）规模部署行动计划>的通知》
央行	金融行业网站	2019年1月10日	《关于金融行业贯彻<推进互联网协议第六版（IPv6）规模部署行动计划>的实施意见》

图 2.1 我国政府部门 IPv6 相关政策文件

1、工信部：明确 IPv6 安全工作阶段性目标

工信部连续两年发布相关政策文件，分阶段细化 IPv6 安全要求。2018 年 5 月，发布《关于贯彻落实<推进互联网协议第六版（IPv6）规模部署行动计划>的通知》，从安全管理、保障措施、安全能力三个维度提出 IPv6 安全总体要求，包括同步升级 IPv6 安全保障系统、强化新兴技术领域安全能力建设等；2019 年 4 月，发布《关于开展 2019 年 IPv6 网络就绪专项行动的通知》，提出 2019 年末 IPv6 安全主要目标，强化落实 IPv6 网络安全保障，如图 2.2 所示。

任务目标	具体要求
安全管理	进一步完善网络安全管理制度体系，涵盖IPv6安全防护和管理相关要求
保障系统	同步升级IPv6网络安全防护手段和监测处置系统
安全防护	加快完成已升级改造的网络和系统单元的网络安全防护工作
标准修订	加快开展IPv6网络安全防护相关标准修订
测试验证	开展IPv6网络安全测试验证，验证已部署的网络安全防护手段有效性
能力强化	开展新兴技术领域IPv6网络安全威胁防范和应对研究

图 2.2 2019 年末 IPv6 安全主要目标

2、广电总局：细化 IPv6 安全指导和安全测试验证要求

广电总局在 2018 年 3 月发布的《广电有线网络 IPv6 规模部署及推进实施指南》中明确细化 IPv6 发展和安全实施指导。其中，在 IPv6 安全方面，该指南从网络攻击、口令攻击、病毒攻击等 9 种 IPv6 安全威胁入手，分析网络侧和业务侧两个方面的 IPv6 安全防护能力，针对终端安全、网络安全、业务安全三个方面，明确提出 IPv6 安全防护策略，如图 2.3 所示。

安全场景	安全策略	具体策略要求
终端安全	针对终端设备制定完善的安全基线要求	针对检测要求、权限设置、API调用等，制修订安全标准等
	建立完善终端恶意软件防范体系	部署恶意软件监测和研判平台、制定恶意代码描述规范等
	提供方便快捷的安全防护服务	建设IPv6终端漏洞库、定期发布终端系统漏洞信息等
网络安全	实施安全域管理机制	根据业务流程、网络功能等划分安全域、制定安全策略等
	提高网络感知能力	在组成端到端网路的各个环节部署探测采集和感知设备等
	提高网络智能决策能力	利用智能管道技术实现高精度流量控制、抑制异常流量等
	提高网络溯源能力	引入合适的溯源方案，如新增日志系统等
	加强网络和设备管理	在网络各节点安装防火墙和杀毒系统实现严格的访问控制等
业务安全	提高业务应用系统鉴权能力	业务提供商采用认证、审计等手段，防止业务盗用等
	加强应用系统漏洞扫描能力	部署漏洞扫描系统，定期开展漏洞扫描和安全评估等
	加强对第三方应用服务器的安全监管	加强对第三方应用服务器平台网络和信息安全监督检查等
	保障IPv6环境下web应用安全	选择满足IPv6环境下IPSec/SSL接入要求的网络设备等

图 2.3 实施指南相关 IPv6 安全防护策略

此外，该指南明确提出在 IPv6 部署过程中同步开展支持能力测试，要求 IPv6 升级改造后的系统应符合国家安全相关标准和行业标准，相关系统上线前应开展安全评测等。

3、教育部：强调 IPv6 安全保障体系总体目标

2018 年 8 月，教育部发布《教育部办公厅关于贯彻落实<推进互联网协议第六版（IPv6）规模部署行动计划>的通知》，明确到 2020 年末基于 IPv6 的安全保障体系基本形成的总体目标，从安全管理、安全设备等方面，强调优化 IPv6 网络安全管理和防护，如图 2.4 所示。

任务目标	具体要求
安全管理	建立健全IPv6网络安全相关制度和技术规范
	开展面向IPv6的网络安全等级保护、风险评估、通报预警
	推进基于流量的安全监测工作，探索真实源地址验证技术的应用
安全设备	完成基于IPv6的安全硬件设备和软件平台的升级改造
	加强网络运行状态监测，留存日志应不少于6个月
安全宣贯	开展管理和技术人员IPv6培训，面向广大师生普及IPv6知识等
安全技术	超前布局安全可信等前沿技术研究，强化网络安全关键技术产学研用协同创新等

图 2.4 教育部 IPv6 安全工作部署

4、央行：同步落实 IPv6 发展和安全工作

央行因其主管的金融服务机构业务特殊性，长期以来十分重视网络安全工作。在 2019 年 1 月发布的《关于金融行业贯彻<推进互联网协议第六版（IPv6）规模部署行动计划>的实施意见》中更是强调金融服务机构 IPv6 升级改造以保障系统安全稳定运行为前提，坚持发展与安全并举，并从主要目标、实施步骤等方面明确提出，按照“初期阶段、规模推广阶段、持续建设阶段”同步推进 IPv6 安全工作。在 IPv6 网络安全保障方面，提出构筑有效防范 IPv6 安全风险且不低于现有 IPv4 同等防护能力的安全防护体系，新增 IPv6 互联网接入线路具备访问控制、入侵检测、流量清洗等安全功能。

此外，国资委在《关于做好互联网协议第六版（IPv6）部署应用有关工作的通知》中，要求各中央企业制定 IPv6 相关任务清单，制定详细工作计划，明确中央企业网站和系统改造计划完成时间，开展 IPv6 环境下移动互联网、物联网、工业互联网等新兴技术研究与应用，同步强化网络安全保障工作的同时，从强化组织领导、保障资金投入、加大扶持力度等方面同步推动 IPv6 发展和安全相关工作。

（二）加快 IPv6 安全科研布局，强化 IPv6 安全技术储备

为防范下一代互联网建设过程中一系列安全风险，我国政产学研各界围绕 IPv6 基础资源安全管理、安全风险应对等问题，开展了一系列 IPv6 安全相关基础科研工作，旨在强化 IPv6 安全技术储备，推动下一代互联网安全演进。

1、强化 IPv6 安全核心要素和基础资源安全管理创新

为强化 IPv6 风险应对技术储备，我国高校、企业、科研机构协同合作，依托科技部国家重点研发计划“宽带通信和新型网络”重点专项，重点开展了 IPv6 环境下基础资源管理核心技术研究，以 IPv6 地址真实性作为网络基础设施的信任锚点，通过互联网体系架构中编制语义、路由控制等核心要素创新，实现大规模网络实体和网络行为关联要素可验证、可管理、可追溯，如图 2.5 所示。

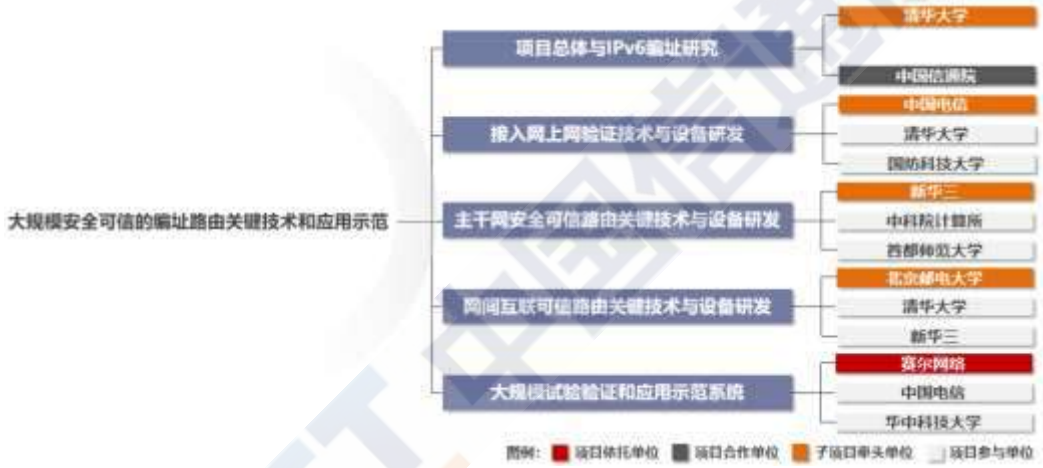


图 2.5 项目组织架构

该项目针对主干网、接入网等不同 IPv6 真实地址部署场景，兼顾开放互通和安全管控，研究提出网络实体、身份、行为的关联机制，从编制语义、路由控制等角度研究实体编址与用户身份、网络行为间的关联关系的同时，构建大规模试验验证和应用示范平台，对自主技术体系、设备系统结构等开展全场景、一体化的验证，强化提升 IPv6 环境下针对 IPv6 地址资源的安全管理能力，如图 2.6 所示。

图 2.6 项目研究框架

2、开展 IPv6 安全风险研究，构建 IPv6 安全应对体系

随着下一代互联网安全问题的逐渐显现，基础电信企业作为我国推动 IPv6 规模部署工作的重要主体，在加快推动网络基础设施、应用基础设施等 IPv6 升级改造的同时，从升级网络安全防护手段、开展 IPv6 网络安全风险研究等方面同步推动 IPv6 网络安全保障工作。其中，中国电信于 2017 年开展 IPv6 网络安全风险相关研究工作，从网络安全防护体系、基础安全风险等方面，梳理 IPv6 安全风险对网络安全防护体系带来的安全挑战，分析过渡技术安全风险、IPv6 新增风险等 IPv6 网络安全相关风险，以及 IPv6 协议机制对自身安全性的影响，形成 IPv6 安全风险框架，如图 2.7 所示。

图 2.7 中国电信 IPv6 安全风险框架

基于该框架中对 IPv6 安全风险的研究分析，针对其各业务场景安全需求，从安全管理、过渡技术、安全设备、访问控制等方面，形成涵盖边界防护、资产管理、威胁情报等内容的 IPv6 安全策略部署建议，如图 2.8 所示。

图 2.8 中国电信 IPv6 安全策略部署建议

3、推动 IPv6 源地址认证和网络攻击追踪溯源研究

清华大学早在 2003 年依托 CNGI 提出真实 IPv6 源地址验证体系结构（SAVA）[13]，旨在通过域间、域内等网络层级的源地址识别和验

[13] 真实 IPv6 源地址验证体系结构：Source Address Validation Architecture，SAVA。

证，对伪造源地址的分组进行过滤，保证网络中所有分组源 IPv6 地址的全网唯一性，进而通过在接入网内和其他不同网络层级上建立不同颗粒度的 IPv6 地址到其他类型标识的绑定关系，将 IPv6 地址逐级定位到网络实体，实现网络攻击行为的可溯源性[14]，如图 2.9 所示。

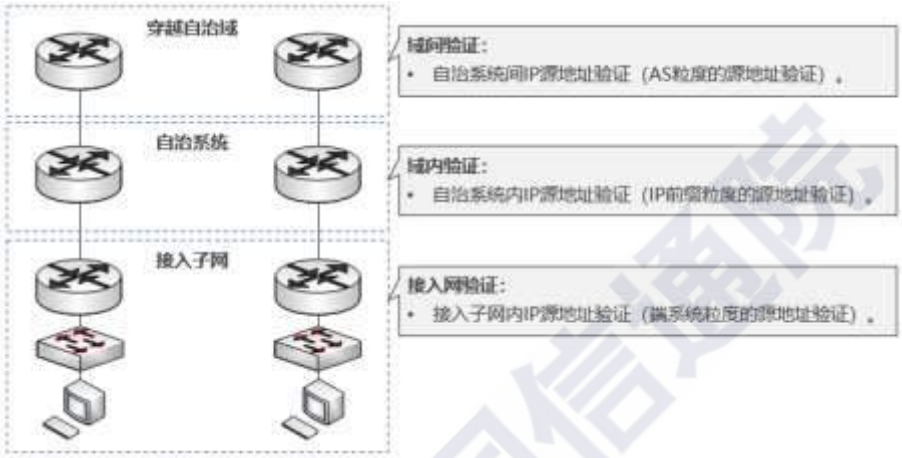


图 2.9 真实 IPv6 源地址验证体系结构体系结构

近年来，清华大学同样依托科技部国家重点研发计划“宽带通信和新型网络”重点专项，持续开展下一代互联网安全相关科研工作，提出“一体化融合网络体系结构和关键技术研究”研究项目，旨在依托 IPv6 网络体系结构，针对空间信息网、广播电视网、移动互联网等多种异构网络的安全高效互联互通面临的技术难题，研究大规模可扩展、时空大尺度、多维高性能、真实安全可信、开放互联融合的一体化新型网络体系结构及其协议关键技术，为未来新型网络的发展奠定理论和技术基础。其中，在下一代互联网安全方面，该项目旨在研究一体化融合网络真实安全可信技术，实现源地址认证、用户身份认证、路由信息认证等功能，构建安全可信的未来一体化融合网络。

[14] 参考文献：李杰，吴建平，徐恪，《自治域间真实源地址验证方法及技术实现》。

（三）推动 IPv6 安全实践，强化 IPv6 安全创新

1、加快 IPv6 安全标准制修订，强化 IPv6 安全指导

从国家标准、行业标准等不同层面，我国标准化组织全面启动 IPv6 安全标准制修订工作，从 IPv6 安全防护、标准体系等方面持续强化 IPv6 安全指导，如图 2.10 所示。

图 2.10 IPv6 安全相关标准工作

国家标准方面，TC260[15]的 WG6[16]聚焦 IPv6 网络安全标准化工作，从国内外 IPv6 发展现状入手，在分析 IPv6 网络安全风险的基础上，研究提出涵盖应用层、网络层、终端层等不同层次的 IPv6 网络安全体系框架，并从基础、技术、管理等方面研究提出 IPv6 网络安全标准化路线图。**行业标准方面，**CCSA[17]主要聚焦 IPv6 环境下多种业务场景网络安全防护要求，以及 IPv6 地址实名制等安全新问题，开展标准制修订工作。其中，TC8[18]的 WG3[19]强化 IPv6 地址申请、分配、备案等安全管理，加快推进 IPv6 地址实名制管理系列标准制定工作。

[15] TC260：全国信息安全标准化技术委员会。
[16] WG6：通信安全标准工作组。
[17] CCSA：中国通信标准化协会。
[18] TC8：网络与信息安全。
[19] WG3：安全管理组。

目前，IPv6 地址实名制管理总体要求、备案信息核查系统技术要求等 5 项标准均已完成报批稿，进入报批审核阶段。NTC4[20]根据 IPv6 环境下引入的网络安全风险，加快推进 IDC、CDN、DNS 等多种业务场景网络安全防护要求标准修订工作。目前，互联网数据中心安全防护相关标准已进入征求意见阶段。

2、加强 IPv6 安全产品和服务探索，助力安全能力提升

从下一代互联网安全需求看，IPv6 环境下协议类型转变、海量地址空间等特性给安全产品功能提出新的要求。一方面，IPv4 向 IPv6 网络升级演进是长期、持续的过程，网络安全产品同时支持 IPv4 和 IPv6 已经成为其部署应用的关键要素。另一方面，基于 IPv6 的下一代互联网自身具有浩瀚的地址空间，也将为网络安全产品带来新的挑战。例如，漏洞扫描类网络安全产品难以在 IPv6 环境下实施遍历式扫描，导致其产品自身基于网络节点扫描发现系统、网络、应用漏洞的工作模式难以高效进行。此外，IPSec 作为 IPv6 环境下可选拓展安全功能，提供端到端加密数据通信机制的同时，也为攻击者规避防火墙、IPS 等网络安全产品的深度分析和检查提供可趁之机。因此，**IPv6 安全产品和服务作为下一代互联网安全防线的核心组成部分，加快其研发、推广、部署已成为保障下一代互联网安全发展的关键**。

我国安全企业加快发力，加快研发升级现有安全产品的 IPv6 支持能力，以及开展 IPv6 环境安全新产品探索。目前，我国已有 231 款

[20] NTC4：网络安全防护特设组。

安全产品通过 IPv6 支持认证[21]，实现对 IPv6 协议层面的支持，产品类型覆盖防火墙、IDS/IPS、UTM、WAF 等，如图 2.11 所示。

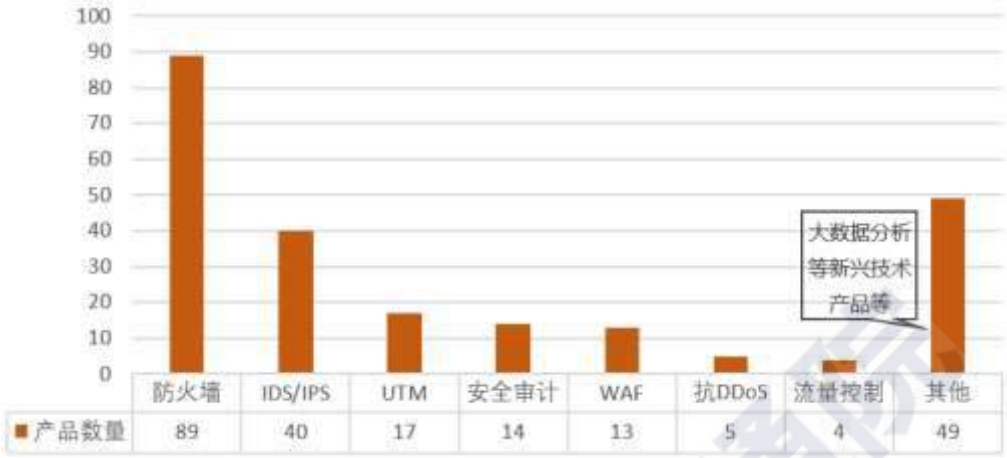


图 2.11 我国通过 IPv6 支持认证的安全产品情况

在 IPv6 安全服务方面，由于 IPv6 网络中传输介质、通信链路、应用系统等关键组成部分与 IPv4 网络基本相同，代码审计、漏洞挖掘等传统安全服务仍将适用于 IPv6 环境。在下一代互联网升级演进过程中，我国安全企业也针对 IPv6 环境相继推出特有安全服务。例如，部分安全企业推出 IPv6 安全改造服务，针对网络和应用基础设施、互联网应用等不同对象，提供 IPv6 安全改造咨询、方案设计等。

3、探索 IPv6 安全解决方案，强化 IPv6 安全风险应对

随着我国下一代互联网建设的持续推进，各类 IPv6 安全事件的出现给下一代互联网安全发展敲响警钟，IPv6 安全问题逐渐引起各界的广泛关注。为提高 IPv6 安全风险防范能力，我国企业从网络基础设施、应用基础设施、基础资源管理等方面，加快开展 IPv6 安全实践和探索，推动 IPv6 安全技术创新和应用，如图 2.12 所示。

[21] 数据来源：下一代互联网国家工程中心《2018-2019 全球 IPv6 支持度白皮书》。

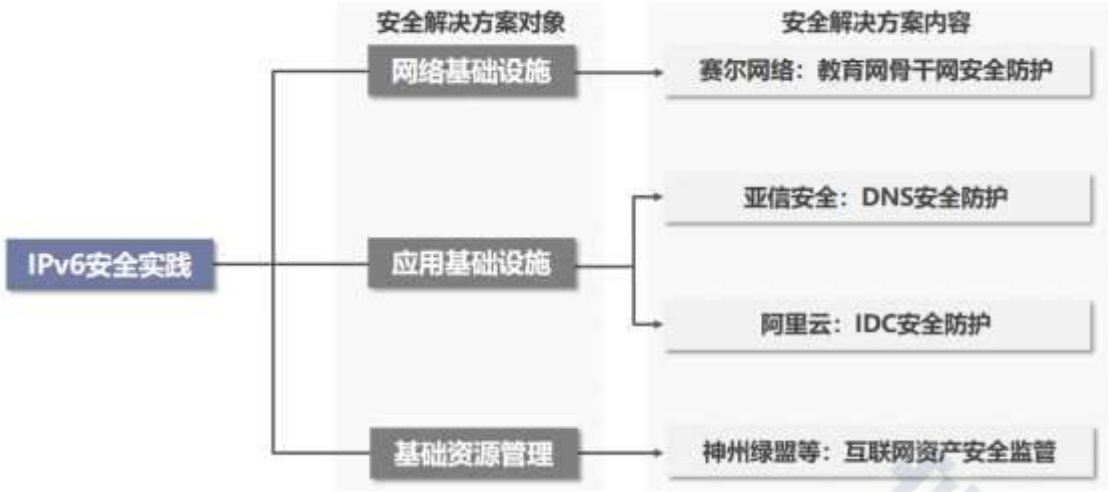


图 2.12 我国 IPv6 安全相关实践

网络基础设施方面，赛尔网络基于 CERNET2 主节点流量采集和分析，优化升级教育网 IPv6 态势监测系统，实现 IPv6 环境下网络攻击监测发现、网络流量分析与监测、安全态势感知等监测预警功能，建设面向云计算与大数据应用的云网一体化安全平台，结合蜜罐态势监测、漏洞自动扫描等网络安全防护系统，实现资产安全管理、数据保护、漏洞检测和防御等网络安全防护功能，保障教育网主干网和纯 IPv6 云平台的云网一体化安全。

应用基础设施方面，亚信安全针对 IPv6 环境下 DNS 面临的 DDoS 攻击、域名安全威胁等问题，提出 DNS 自适应安全架构，依托企业自身威胁情报库中 IPv6 地址黑名单，结合 DNS 流量监测分析系统，对访问 DNS 的源 IP 以及域名解析 IP 实施预测分析，同时按照 DNS 安全策略，通过安全防护设备实施深度检测并阻断非法 IP 访问，形成预测、防御、检测、响应的 DNS 安全防御闭环。阿里云针对 IPv6 环境下 IDC 开展 DDoS 防护安全实践，采用分布式计算、全链路双栈等技术，构建 IPv6 环境下 DDoS 防御系统，以及 SaaS 化的 DDoS

防御产品，保障企业自身业务安全的同时，可为互联网企业提供 IPv6 环境下 DDoS 安全防护产品和服务。

基础资源管理方面，神州绿盟等企业针对 IPv6 海量互联网资产难以实施高效的扫描、监测等问题，加快构建 IPv6 环境下互联网资产发现、识别、管理等安全能力，结合大数据分析等网络安全技术，满足 IPv6 环境下互联网资产安全监测、风险评估、威胁预警、应急处置等安全需求，切实提升 IPv6 环境下互联网资产网络安全管理能力。

值得注意的是，由于我国互联网应用 IPv6 升级改造进度相对滞后，目前针对互联网应用的 IPv6 安全实践屈指可数。未来随着互联网应用 IPv6 升级改造进度的不断提升和需求市场的逐步扩大，可以预见将有更多企业针对互联网应用开展 IPv6 安全相关创新实践。

三、我国下一代互联网建设仍面临的安全挑战

IPv6 凭借其浩瀚的网络地址空间，能够有效解决当前全球互联网面临的网络地址消耗殆尽等网络发展瓶颈问题。然而，IPv4 向 IPv6 网络升级演进是一个长期、持续的过程，IPv4/IPv6 过渡机制以及 IPv6 协议新特性带来的客观安全问题不容忽视。此外，目前已部署上线的 IPv6 业务相对有限，IPv6 安全产品和服务发展、IPv6 安全保障能力的建设也相对滞后，我国下一代互联网建设仍面临现实安全挑战。

（一）IPv4/IPv6 长期并存，过渡机制持续叠加安全风险

如前所述，在下一代互联网建设过程中，IPv4 网络和 IPv6 网络

将长期并存，为保障 IPv4 和 IPv6 网络间的相互通信，通常采用双栈、隧道、翻译等过渡机制实现向纯 IPv6 网络的平稳升级。然而，部分过渡机制自身存在安全缺陷，或将引入新的安全隐患，导致下一代互联网建设过渡期安全风险持续叠加。

1、双栈机制：IPv4/IPv6 网络安全暴露面倍增

双栈机制是指网络节点同时具备 IPv4 和 IPv6 两种协议栈，具备两种协议的支持能力。在双栈环境下，源节点根据目的节点协议栈类型选择不同的协议栈封装和发送报文，网络设备根据接收到的报文协议类型，选择不同的协议栈对报文进行处理和转发，如图 3.1 所示。

图 3.1 双栈机制原理

在双栈环境下，采取 IPv4 和 IPv6 并存的通信模式，因 IPv4、IPv6 中任何一种协议安全漏洞等问题引发的不良影响将会以网络设备等为据点，在 IPv4 和 IPv6 网络中双向渗透传播，无形中增加网络节点的安全暴露面。例如，攻击者可利用 IPv6 协议栈漏洞，针对双栈环境下网络设备发起 DDoS 攻击，进而影响网络设备正常工作，引发 IPv4 和 IPv6 网络均无法正常访问，如图 3.2 所示。

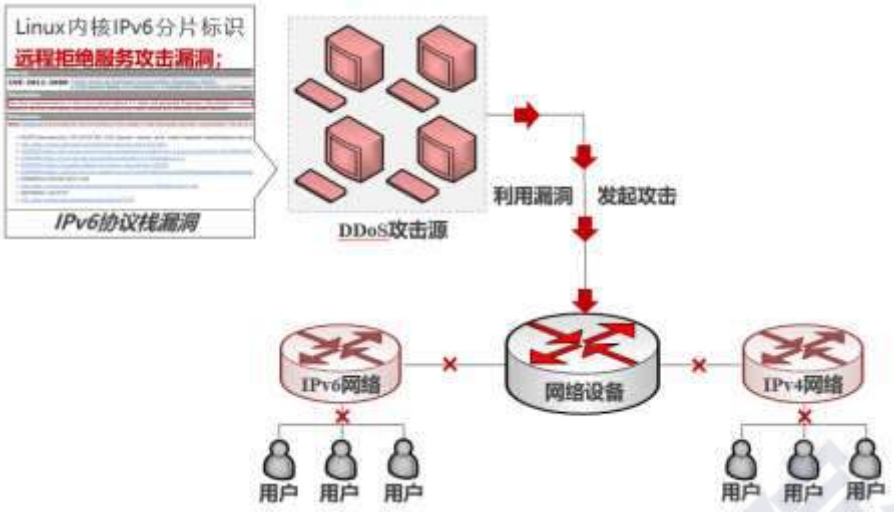


图 3.2 双栈机制安全风险

2、隧道机制：内置安全功能缺失，安全影响范围扩大

隧道机制可实现 IPv6 数据包在 IPv4 网络中传输，其核心在于将 IPv6 数据包封装在 IPv4 数据包中，以自动、手动等多种隧道配置方式，保障被 IPv4 网络隔离开的局部 IPv6 网络间相互通信。以 IPv6 to IPv4 和 IPv6 over IPv4 为例，地址格式如图 3.3 所示。

图 3.3 常见隧道机制地址格式

在隧道环境下，部分隧道机制仅要求隧道出入口节点对报文进行简单的封装和解封，缺乏内置认证、加密等安全功能，导致攻击者可能截取隧道报文，伪造用户地址并伪装成合法用户发起攻击。以 IPv6 over IPv4 为例，攻击者可伪造内层、外层地址发起仿冒攻击等安全风险。此外，由于部分隧道机制未采取对隧道封装内容的检查，攻击者

可通过隧道封装攻击报文，导致攻击流量可通过隧道向其他网络辐射，形成隧道化的攻击模式，如图 3.4 所示。

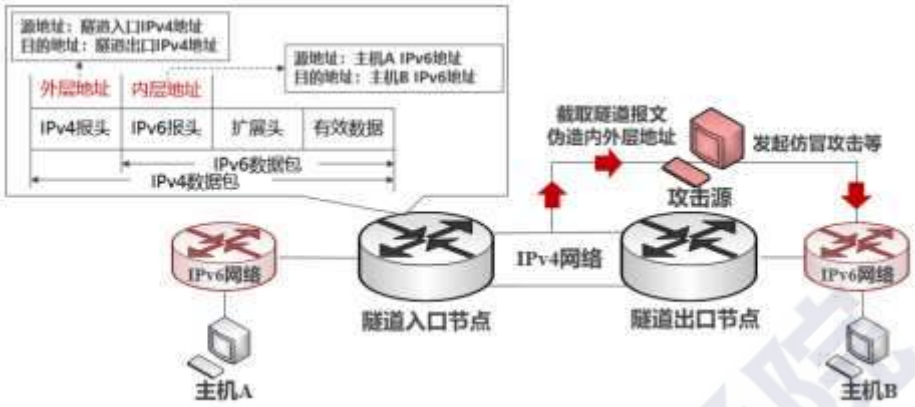


图 3.4 隧道机制安全风险

3、翻译机制：机制内在特性仍面临传统网络攻击威胁

IPv4/IPv6 过渡期通常采用网络地址转换（NAT）[22]技术实现 IPv4 和 IPv6 地址间的相互转换。与 IPv4 环境下[23]不同，在 IPv4/IPv6 过渡期，NAT 技术可实现 IPv4 地址和 IPv6 地址间的双向映射，通过翻译节点实现 IPv4 和 IPv6 地址间的相互转换。由于 IPv4 地址紧缺的现象仍客观存在，IPv4 地址与 IPv6 地址间的一对一映射将造成 IPv4 地址资源的浪费，目前主流的技术方案通常采用 IPv4 地址和端口号与 IPv6 地址间映射的方式[24]，在节约 IPv4 地址资源的同时，保障 IPv4 和 IPv6 网络间相互访问，如图 3.5 所示。

[22] 网络地址转换：Network Address Translation，NAT。
[23] 在 IPv4 环境下，通常采用 NAT 技术将一个公有 IPv4 地址映射为多个 IPv4 内网地址，实现外网与内网间 IPv4 地址相互转换。
[24] 因 IP 端口号共有 2^{16} 个，故一个 IPv4 地址最大支持映射 2^{16} 个 IPv6 地址。

图 3.5 翻译机制原理

目前，由于 IPv6 相关业务尚未大规模部署上线，仍存在大量主机通过翻译机制访问 IPv4 网络资源。尽管翻译机制在 IPv4/IPv6 过渡期与在 IPv4 环境中作用不同，但机制特性仍未发生改变，同样面临地址池耗尽等常见 DDoS 攻击威胁，攻击者可通过伪造大量 IPv6 地址向翻译节点发起地址转换请求，消耗地址池 IPv4 资源，同时导致合法用户无法获取 IPv4 地址，进而引发 IPv4 网络无法正常访问，如图 3.6 所示。

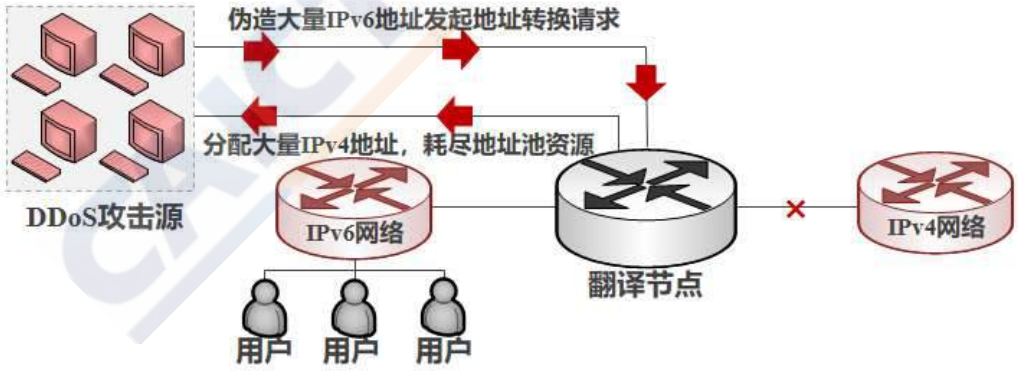


图 3.6 翻译机制安全风险

总体来看，在 IPv4 网络向 IPv6 网络升级演进期间，双栈、隧道等过渡机制均需针对机制特性，配备针对性的网络安全防护机制。值得注意的是，翻译机制在 IPv4 环境中已形成相对成熟、可沿袭的网络安全防护机制，且在真实网络环境已经过较长时间的有效性验证，

仅需针对翻译节点设备部署源地址认证等安全防护策略，如图 3.7 所示。因此，**相对坚实的安全保障基础使得翻译机制或将成为 IPv4/IPv6 过渡机制的首选。**

过渡机制	安全影响	攻击风险	安全优势
双栈机制	网络和风险并存	因一种协议栈安全隐患引发的各类攻击等	无
隧道机制	内置安全功能缺失	仿冒、泛洪攻击等	无
翻译机制	未改变机制内生特性	地址池耗尽攻击等	已具备成熟的安全防护机制 仅需针对翻译节点设备部署安全防护策略

图 3.7 IPv4/IPv6 过渡机制安全性对比分析

（二）协议新特性挑战现有安全手段，融合场景风险持续扩大

1、IPv6 地址标识复杂性骤增，挑战基于地址资源安全防护手段

网络地址标识泛指网络节点协议类型、地址格式等各类标志信息。尽管 IPv6 能够有效解决全球互联网地址紧缺问题，但协议类型、地址空间、地址格式、掩码格式等网络地址标识的变化，也导致 IPv6 网络中网络地址标识相对于 IPv4 网络地址标识而言，复杂性急剧增加，如图 3.7 所示。

图 3.7 网络地址标识复杂性对比

在 IPv6 网络地址标识复杂性持续叠加的情况下，流量清洗、数据包过滤、入侵检测等以各类网络地址标识解析为核心的传统安全防护手段将面临严峻安全挑战。复杂网络地址标识和海量流量带来的双重压力使得 DPI[25]、防火墙、IDS/IPS[26]等传统安全设备压力急剧增加，难以以 IPv4 环境下相同时间完成复杂网络地址标识解析和规则匹配等安全防御工作，如表 3.1 所示。

表 3.1 IPv6 网络地址标识对安全防护手段的影响

安全技术	影响设备	主要部署场景	安全影响
流量解析	DPI、抗 DDoS	CDN、IDC 防护等	影响对攻击流量实时清洗能力
数据包过滤	防火墙	云、CDN、IDC 防护等	存在虚假数据包跨越的可能
标识解析和规则匹配	IDS、IPS、WAF	云、CDN、IDC、网站防护等	影响对入侵事件识别和发现效率

具体包括：

- **流量解析：**流量解析和清洗是针对 DDoS 攻击的重要安全防御手段之一，可基于网络关键点报文报头中协议类型、目标地址等网络地址标识，实现对异常攻击流量的识别、过滤、清洗等功能。IPv6 环境下，由于网络地址标识复杂程度持续叠加，原本针对 IPv4 环境下相对简单的网络地址标识的流量清洗，需转变为对海量攻击流量中复杂地址标识的解析和匹配工作，导致现有相关安全设备工作耗时剧增，难以进行实时/准实时的分析和清洗。

- **数据包过滤：**数据包过滤作为包过滤型防火墙的主要功能，通过对数据包内各类网络地址标识的检测，可识别和丢弃具有欺骗性源

[25] DPI：Deep Packet Inspection，深度报文检测。
[26] IDS/IPS：Intrusion Detection Systems/ Intrusion Protection Systems，入侵检测系统/入侵防御系统。

IP 地址的数据包。IPv6 环境下，包过滤型防火墙需在短时间内根据各类数据包中复杂网络地址标识进行准确分析和判断，而网络地址标识复杂性的变化，导致防火墙设备压力剧增，尤其是防火墙需建立针对海量地址空间中 IPv6 地址前缀的访问黑名单等，一旦存在遗失遗漏的情况，可能引发虚假数据包穿透防火墙，进而造成不良影响。

- **标识解析和规则匹配：**IDS/IPS 等设备往往根据安全策略定义，基于网络地址标识等报文信息的检测分析，实现对网络攻击事件的识别和发现。IPv6 环境下，要求 IDS/IPS 设备在短时间内根据报文信息中复杂的网络地址标识对网络攻击入侵事件进行准确分析和判断，而网络地址、协议类型等网络地址标识的变化，导致报文信息收集和分析时间剧增，可能因复杂的网络地址标识引发网络攻击入侵事件难以准确判断，影响对网络攻击入侵事件的有效识别和发现。

2、IPv6 协议新特性引入新安全问题，网络安全风险此消彼长

IPv6 协议引入报文扩展头、地址自动配置等新特性，在提高网络服务质量的同时，也引入组播通信、MTU[27]路径发现等新特性，可有效应对广播风暴、分片攻击等部分网络安全风险。然而，由于部分协议新特性未配备适当的安全机制，可能引发扩展头攻击、NDP 攻击等新型网络攻击威胁，导致 IPv6 环境下网络安全风险此消彼长，具体包括：

- **扩展头攻击：**IPv6 协议通过引入报文扩展头，通过将 IPv6 协

[27] MTU：Maximum Transmission Uni，最大传输单元。

议选项字段集中在扩展头中，使得转发设备可根据选项字段选择性处理报文，有效提高报文转发效率。但协议中未限制报文扩展头总数和同类型扩展头出现次数，攻击者可通过构造包含异常数量扩展头的报文，对网络中防火墙、路由器等节点发起 DoS 甚至 DDoS 攻击，迫使相关节点耗费大量资源解析异常数量的扩展头，如图 3.8 所示。

图 3.8 扩展头攻击

- NDP 攻击：IPv6 网络中采用 NDP[28]取代 IPv4 网络中 ARP 和 ICMPv4 部分控制功能，通过在网络节点间交换信息报文实现链路层地址发现、地址自动配置、路由前缀发现等功能。但是，由于 NDP 未配备有效的源节点安全认证机制，可引发仿冒攻击、泛洪攻击等安全威胁，如图 3.9 所示。

图 3.9 NDP 攻击

[28] NDP：Neighbor Discovery Protocol，邻居发现协议。

- **DAD[29]攻击：**DAD 是指网络节点配置 IPv6 地址时，依托 NDP 中 NA[30]、NS[31]报文，预先进行地址重复性检测，以保障该节点获取的 IPv6 地址的唯一性。然而，DAD 过程未配备 NA 报文合法性验证机制，攻击者可监听 DAD 过程，在监听到 NS 报文时，伪造并发送 NA 报文，宣称该 IPv6 地址已被占用，影响 IPv6 地址正常配置过程，进而导致合法节点无法正常访问网络，如图 3.10 所示。

图 3.10 DAD 攻击

- **前缀欺骗攻击：**在 IPv6 地址自动配置过程[32]中，网络节点可监听 RA 报文[33]，根据 RA 报文中路由前缀与自身接口 ID 生成 IPv6 地址，提高 IPv6 地址配置效率。该过程未对源地址进行安全认证机制，攻击者可通过伪造并发送虚假 RA 报文，影响合法节点获取有效 IPv6 地址；也可结合 DAD 攻击，在阻碍节点正常获取 IPv6 地址的同时，伪装成链路默认路由，实施中间人攻击等攻击手段，如图 3.11 所示。

[29] DAD：Duplicate Address Detection，重复地址检测。
[30] NS：Neighbor Solicitation，邻节点请求。
[31] NA：Neighbor Announcement，邻节点公告。
[32] 另一种地址自动配置方式通过路由请求报文（Router Solicitation，RS）获取路由前缀。
[33] RA：Router Advertisement，路由广播。

图 3.11 前缀欺骗攻击

- MLD[34]**攻击**：MLD 具有组成员管理功能，是实现 IPv6 组播高效数据交互的基础。路由节点可依托 MLD 协议识别和发现链路组成员，记录和维护组播信息。但是，MLD 缺少安全认证机制，攻击者可冒充组播源，伪造和发送虚假组播数据，或伪装成组成员，向组播源发送大量虚假的组成员报告报文，消耗组播源内部资源，影响组成员间正常数据交互。

3、IPv6 融合场景放大新技术安全隐患，加剧安全防御被动局面

当前，5G、物联网、工业互联网等新一代信息通信技术和新业态的快速发展应用，在未来构建物物互联的泛在连接场景中，将与 IPv6 地址紧密绑定、与 IPv6 技术深度融合，可能放大新技术新业态本身及应用过程中存在的安全隐患，加大网络安全管理难度。**从网络安全防御方看，**为保障海量互联网资产安全，网络安全防御方需将各类终端、设备等海量互联网资产全面纳入网络安全管理范畴，面对急剧扩张的攻击暴露面，确保海量复杂地址标识的解析、识别和安全分析等

[34] MLD：Multicast Listener Discovery，组播侦听发现。

工作万无一失。**而从网络攻击方看**，仅需在偌大的攻击面中发现一个或多个脆弱点作为突破口，即可发起针对性的攻击并向更深更广的范围渗透。防守方需“知其全貌”而攻击方只需“知其一二”的**攻防不对称的局面进一步加剧**。

例如，在 IPv6 与 5G、物联网等新技术融合应用的海量机器类通信（mMTC）场景中，数以百亿计的各类物联网终端、设备等资产将直接暴露在互联网上。由于物联网资产本身存在的安全漏洞、数据泄露、非授权接入等安全风险不可避免，若未对所有资产实施恰当的安全管理，攻击者嗅探发现其一二进而入侵利用后，可构造规模化的设备僵尸网络并发起新型高容量 DDoS 攻击，导致安全威胁向用户应用和核心网络双向辐射，如图 3.12 所示。

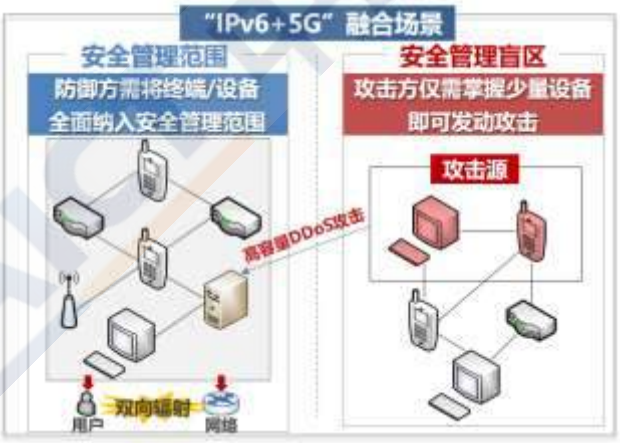


图 3.12 IPv6 与 5G 融合场景安全风险

（三）IPv6 网络安全需求能力“剪刀差”亟需弥合

1、IPv6 安全产品发展尚在起步，远滞后安全能力需求

随着 IPv6 相关网络安全问题逐渐引起重视，国内安全企业同步加快 IPv6 安全产品的研发推广。但就现阶段 IPv6 相关安全产品的研发应用情况来看，目前市场对 IPv6 安全产品发展的驱动效应尚未全

面显现，我国 IPv6 安全产品仍处于起步发展阶段，如图 3.13 所示。

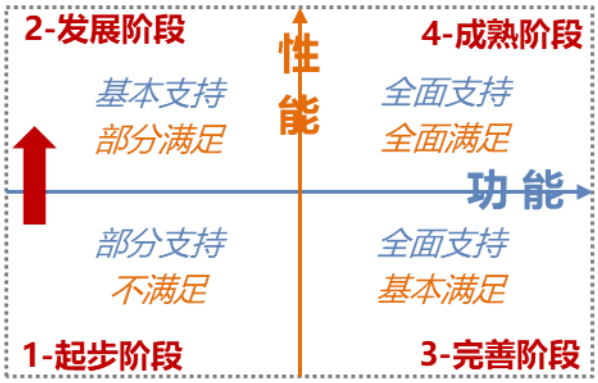


图 3.13 IPv6 安全产品发展和成熟度象限

- **IPv6 安全产品起步阶段：**少量安全产品在功能上可支持 IPv6 协议，包括支持 IPv6 地址解析、IPv6 报文分析等，但未付诸实际部署应用过程，在 IPv6 环境下的安全防护性能和防护效果未得到验证。

- **IPv6 安全产品发展阶段：**市场驱动的良性发展效应初显，主流安全产品基本支持 IPv6 协议，以防火墙、WAF 等为代表的典型安全产品可在 IPv6 环境下具备相对良好的安全性能。

- **IPv6 安全产品完善阶段：**安全产品全面支持 IPv6 协议，并在 IPv6 环境下得到部署应用，安全产品防护性能和防护效果可满足 IPv6 环境下的安全防护要求。

- **IPv6 安全产品发展成熟阶段：**IPv6 安全产品具备相对完善的功能性能，并与大数据分析、人工智能等安全赋能技术深度融合，实现安全产品核心技术创新突破和防护效能质的提升。

总体来看，现阶段尽管我国以防火墙、WAF、IDS/IPS 等为代表的安全产品已加紧支持 IPv6 协议解析等基本功能，但在支持产品功能多样性、产品性能等方面，仍滞后于 IPv6 环境下的安全能力需求，

特定类型的安全产品缺失也将对下一代互联网建设过程中的安全保障带来深远影响，如表 3.2 所示。

表 3.2 常见安全产品缺失对 IPv6 安全保障工作的影响

安全产品	缺失影响
防火墙	基础防御屏障缺失
抗 DDoS	高容量 DDoS 攻击应对能力不足
IDS/IPS	无法有效识别、响应、处置 IPv6 攻击入侵事件
WAF	网络应用安全难以保障，难以防御典型 Web 攻击
身份识别与访问控制	无法实施有效的用户身份识别和网络信息管理
漏洞扫描	缺乏自动化的漏洞识别和发现能力
安全审计	难以有效追踪发现 IPv6 异常事件

2、IPv6 安全问题未充分暴露，制约安全服务发展步伐

在 IPv4 环境下，依托代码审计、漏洞挖掘等网络安全服务能有效发现和识别企业业务开发、运维等各环节存在的安全隐患，助力企业安全能力提升。目前，我国基础网络、政企和商业网站等已具备各项 IPv6 业务支持能力，但 IPv6 网络和应用仍未大规模投入使用，导致 IPv6 安全问题未充分暴露，现有网络安全服务 IPv6 验证环境的缺失也将导致 IPv6 应用代码缺陷、安全漏洞等安全问题不能得到全面和深入的验证，如表 3.3 所示。

表 3.3 常见安全服务缺失对 IPv6 安全保障工作影响

安全服务	缺失影响
安全集成	系统工程建设过程中违规行为无法发现，埋下未知安全隐患
运维服务	难以发现 IPv6 网络、应用、设备中可能存在安全管理风险
维保服务	难以发现 IPv6 设备安全管理风险
代码审计	难以发现 IPv6 相关应用中可能存在代码设计缺陷
教育培训	相关工作人员 IPv6 安全知识技能难以得到有效提升
渗透测试	难以有效识别和发现 IPv6 相关资产潜在安全漏洞等隐患
漏洞挖掘	
风险评估	

3、“IPv6+网络安全”复合型专业技术人才缺失

当前，我国网络安全学科教育年度培养规模约 1 万人左右，且普遍存在从业人员知识储备、技能等方面短板，重要行业和领域网络安全运维保障、监管执法等人才短缺等现实问题[35]。在网络安全人才紧缺的大背景下，**一方面，IPv6 新环境下网络安全专业人员正面临严峻挑战。**IPv6 环境下引入扩展头攻击、NDP 攻击等安全新威胁，给企业安全技术人员带来新的挑战。安全专业人员的 IPv6 知识储备不足，将引发无法充分认识和理解 IPv6 安全问题，无法有效应对 IPv6 安全防护需求等现实问题。**另一方面，大量运维人员缺乏 IPv6 安全相关知识和经验。**尽管我国早在 2003 年已将 IPv6 发展提上日程，但早期对 IPv6 的研究多集中在教育网等相对封闭的环境中，企业运维人员未能第一时间接触 IPv6 业务运营、维护等实际业务环境，现有 IPv4 安全知识和经验难以直接应用到 IPv6 环境中，导致 IPv6 相关业务的运维工作存在安全隐患，大量弱防甚至不设防的 IPv6 协议栈成为攻击者实施网络攻击的新突破口。

四、保障下一代互联网安全有序发展的建议

我们正处于全球信息通信技术加速创新变革、信息基础设施加速演进升级的战略机遇期。加快推进 IPv6 规模部署，构建高速率、广普及、全覆盖、智能化的下一代互联网，已成为我国实现网络技术突破、基础设施升级和应用服务创新的关键举措。我国在大力推动下一

[35] 参考文献：《网络安全产业白皮书（2018）》。

代互联网建设的同时，已同步开展 IPv6 网络安全保障工作。尽管 IPv6 网络安全风险逐渐显现，但我国下一代互联网建设新环境下网络安全攻防也大体处于同一起跑线，IPv6 安全挑战和机遇并存的局面已经形成。因此，未来应高度重视下一代互联网的演进升级过程中出现的安全新挑战，加快构建各方参与、有机互补的协同工作机制，联合我国政产学研多方力量，**加快推动 IPv6 安全产品和服务研发、推广、部署、应用，为筑牢下一代互联网安全防线提供核心能力保障**，建立创新发展机制、加强专业人才实力，加快形成下一代互联网安全防御闭环，切实保障下一代互联网安全、有序发展，如图 4.1 所示。

图 4.1 IPv6 网络安全协同工作机制

（一）主动布局 IPv6 安全产品服务和安全实践推广

有效、可靠的安全产品和服务是筑牢下一代互联网安全防线的关键基石。**安全企业应加快主动布局 IPv6 安全产品服务，推动 IPv6 安全实践研发推广**，针对性地强化 IPv6 安全保障能力，如表 4.1 所示。

表 4.1 加快研发推广的 IPv6 安全产品和服务清单

类别	细分类别	产品/服务	IPv6 环境下安全功能升级
安全产品	安全防护	防火墙	支持 IPv6 安全策略配置，IPv6 数据量监测、分析和过滤，IPv6 网络内部结构、运行状况信息屏蔽等
		IDS/IPS	识别和防御 IPv6 网络攻击入侵事件
		WAF	IPv6 数据包分析校验，用户请求扫描过滤，异常数据包阻断隔离等
		漏洞扫描	IPv6 安全漏洞自动化识别和发现
		抗 DDoS	IPv6 网络攻击流量的识别和过滤
安全服务	安全集成	安全集成服务	一站式 IPv6 安全升级改造服务
	安全运维	运维服务	IPv6 安全评估、监控和安全响应等
		维保服务	IPv6 安全设备的故障排除、隐患排查和组件更换等
		渗透测试	IPv6 网络、系统、应用等漏洞的探测挖掘
	安全咨询	教育培训	针对 IPv6 的安全知识和技能培训

在安全产品方面，

- **防火墙：**作为 IPv6 环境下基础安全屏障，是下一代互联网安全防线的核心组成部分。防火墙可借助软硬件作用于 IPv6 网络间，通过监测、限制、处置跨越防火墙的数据流，对内根据安全策略配置过滤 IPv6 环境下非法数据流，实现对风险连接的访问阻断，对外屏蔽 IPv6 网络内部结构、运行状况等信息，保障 IPv6 环境下内部网络与外部网络、专用网络与公共网络间隔离和安全。此外，IPv4/IPv6 过渡期翻译机制成熟的安全防护策略也需依托防火墙配置，实现过渡期安全防护相关功能。

- **IDS/IPS**：面临 IPv6 网络攻击事件时，对攻击入侵活动的识别和防御尤为重要。IDS/IPS 可对网络活动进行实时监测，在从网络关键节点收集网络、系统、用户等相关信息的基础上，通过模式匹配、统计分析等技术手段对收集到的信息进行分析，发现和识别已知 IPv6 攻击入侵活动等异常网络行为，进而中断、隔离异常网络行为，具备入侵防护、流量控制等多种安全功能的同时，可根据异常网络行为的性质、类型等特征，做出相应的告警、响应、处置等。

- **WAF**：海量行业网站是 IPv6 升级改造的重要对象，在全面支持 IPv6 访问的同时，也对 IPv6 环境下网站安全防护提出新需求。WAF 作为网站应用安全防护屏障，可通过特征提取和分块检索技术进行特征匹配，提供针对 HTTP /HTTPS 访问 Web 应用等安全防护功能，在用户请求到达 Web 服务器前，进行扫描和过滤，分析校验相关数据包，对异常数据包进行阻断或隔离，确保每个用户请求有效且安全，可有效防范 IPv6 环境下 Web 应用攻击、DDoS 攻击等。

- **漏洞扫描**：基于漏洞数据库、特征库等，通过远程、本地等扫描方式，对网站、主机、端口、应用等安全脆弱性进行检测，发现和识别已知安全漏洞，指导针对网络和系统单元快速掌握安全状态、修复相关漏洞。随着 IPv6 相关业务的相继部署上线，IPv6 安全漏洞也将呈现出逐渐增多的趋势，对 IPv6 安全漏洞的自动化扫描和修复，将成为识别发现潜在网络安全隐患、切实提高网络安全防护能力关键。

- **抗 DDoS**：尽管防火墙、IDS/IPS 等安全设备自身已具备 DDoS 攻击安全防护功能，但多通过控制数据访问速率、随机丢弃数据包等

形式，存在因设备负荷压力剧增导致无法正常工作的可能。未来，随着 IPv6 业务的相继部署上线，IPv6 网络攻击事件逐渐显现的同时，IPv6 网络攻击流量将持续增长，抗 DDoS 安全产品本身具备强负荷环境下高效的 DDoS 攻击防范能力，在面对 IPv6 环境下高容量 DDoS 攻击时具有天然的安全防护优势。

在安全服务方面，

- **安全集成服务：**采用技术整合、功能整合、数据整合、模式整合、业务整合等技术手段，将各个分离的设备、软件和信息数据等要素集成到相互关联的网络信息系统中，使系统安全功能和性能符合使用要求，实现集中、高效、便利的安全管理。随着 IPv6 规模部署工作的持续推进，系统集成服务相关机构可提供一站式 IPv6 安全升级改造服务，助力海量网站和系统加快开展 IPv6 升级改造工作。

- **运维服务：**对委托安全运维服务的企业涉及的网络、应用、设备等不同主体进行安全管理，主要包括安全评估、监控、安全响应等，以降低安全隐患发生可能性，提高安全事件应急响应能力。现阶段，由于企业运维人员相对缺乏 IPv6 安全知识和技能，选择合适的 IPv6 安全运维服务或将在一段时间内成为企业保障 IPv6 业务安全的关键。

- **维保服务：**企业购买维保服务后，通过远程、驻场等方式对维保期内的网络和安全设备涉及的软硬件提供技术支持，服务主要内容包括故障解除、隐患排查、组件更换等，降低设备故障对业务的影响，满足设备高效、稳定的运行需求。在企业开展 IPv6 升级改造过程中，新部署应用的网络和安全设备具备支持 IPv6 的能力的同时，也将为

IPv6 网络和安全设备的维保服务发展带来契机。

- **渗透测试：**渗透测试是依托第三方服务机构的安全技术人员，针对服务网络和系统进行入侵事件进行模拟演练的一种网络安全服务形式。随着 IPv6 相关网络和系统的相继上线，渗透测试可通过模拟攻击行为对新上线的 IPv6 网络和系统进行探测和挖掘，识别和发现安全隐患，测试和验证安全防护能力，形成渗透测试结果，助力提升 IPv6 环境下网络和系统安全能力。

- **教育培训：**主要包括安全技术教育培训、安全管理教育培训等多种形式，旨在提升相关工作人员网络安全知识水平和技术能力，规范企业业务开发、运行、维护流程，降低发生网络安全事件的可能的同时，强化各类安全事件技术应对能力，尤其是针对现阶段 IPv6 专业技术人才缺失现状，IPv6 安全教育培训已经成为提升相关人员安全知识技能不可或缺的环节。

（二）按需求、分场景落实 IPv6 安全产品服务部署

企业应结合自身网络和业务场景的 IPv6 安全需求，加快 IPv6 安全产品和服务部署应用，落实按需求、分场景的精细化 IPv6 安全防护体系，如图 4.2 所示。

安全产品和服务类别		典型业务场景						融合应用场景	
		骨干网络	LTE 网络	IDC	CDN	DNS	云	5G 融合	物联网融合
安全产品	防火墙	△	△	△	√	√	√	△	△
	IDS/IPS	△	△	√	√	√	√	△	△
	WAF	●	●	√	●	●	√	●	●
	漏洞扫描	●	●	△	△	△	△	△	√
	抗 DDoS	△	△	√	√	√	√	√	√
	身份识别与访问控制	△	√	△	△	△	√	√	√
	安全审计	△	△	△	√	△	√	√	△
安全服务	安全集成服务	●	●	●	△	√	●	●	●
	运维服务	●	●	√	△	√	●	△	△
	维保服务	●	●	●	△	●	●	●	●
	渗透测试	√	√	△	●	●	●	√	√
	风险评估	△	△	△	√	√	√	√	√
	代码审计	√	√	△	●	△	●	√	√
	漏洞挖掘	●	●	√	●	●	●	△	△
	教育培训	△	△	△	√	△	√	√	√

图例：√增强安全防护措施　　△基本安全防护措施　　●可选安全防护措施

图 4.2 场景化 IPv6 安全防护措施落实表

其中，IPv6 环境典型业务场景重点安全需求包括：

- **骨干网业务场景：**作为承载各项互联网业务的动脉，骨干网络由路由、网关等各类硬件设备组成。当前，骨干网 IPv6 安全防护能力仍处于同步建设阶段，一旦硬件设备遭受网络攻击或存在安全问题，将直接影响 IPv6 相关业务的安全开展，可能引发“一点突破、全网皆失”的严重后果，硬件设备安全已成为保障骨干网络安全核心因素。

- **LTE 网络业务场景：**与骨干网络类似，目前针对 LTE 网络的 IPv6 升级改造依托核心网相关设备进行，硬件设备安全同样是保障 LTE 网络安全的关键。此外，LTE 网络存在海量移动终端，由于无线通信链路的脆弱性，可能存在非法接入、仿冒攻击等安全风险，应同样重视因移动终端安全隐患引发的 LTE 网络安全风险的防范和应对。

- **IDC 业务场景：**随着 IPv6 升级改造工作持续推动，IDC 数据信息海量化、存储服务集约化等特点也将逐渐向 IPv6 环境迁移。同时，作为海量数据存储、交互的中心，IPv6 环境下 IDC 可能面临来自内部和外部的网络攻击，尤其需要对 DDoS 攻击、Web 类应用被挂马、蠕虫病毒入侵，以及由于对 IDC 网络进行维护不恰当等原因导致的安全风险进行重点应对。

- **CDN 业务场景：**随着互联网应用相继完成 IPv6 升级改造，视频、直播等大流量业务逐步部署上线，CDN 凭借其静态、动态内容加速服务功能，可保障大流量业务的高效开展。在 IPv6 环境下，系统部署防入侵防攻击措施不到位，可能导致攻击者从外网渗透进内网系

统；请求路由系统的域名解析安全机制缺陷，也可能引发 CDN 分发信息被劫持或重定向等。此外，动态内容通常仍由源服务器存储，在传输过程中由于缺乏适当的安全机制，可能被注入攻击流量，应着重强化针对 CDN 的流量型攻击应对能力。

- **DNS 业务场景：**在 IPv6 环境下，DNS 在向用户主机返回域名解析结果的同时，也会在日志中记录存储海量用户主机/联网终端的真实 IPv6 地址[36]，因此，攻击者若想获得用户地址，将选择 DNS 作为 IP 地址扫描探测的首选目标[37]，对其实施入侵破解、DDoS 攻击、DNS 缓存投毒等针对性的攻击手段。

- **云平台业务场景：**目前，各行业领域存在海量网站依托云托管的模式开展 IPv6 升级改造工作。随着云托管网站 IPv6 升级改造工作的相继完成，云平台面临的来自应用、网络等层面的安全威胁将逐渐凸显，其安全问题也将持续辐射延伸，造成云托管网站无法正常访问等不良影响，云平台安全能力已成为新环境下保障网站安全的关键。

典型新技术融合场景安全需求具体包括：

- **5G 融合应用场景：**5G 应用场景中，硬件、应用、网络等层面本身存在安全风险，例如，海量终端设备存在的安全认证风险、多种传输模式带来的网络攻击风险、业务开放能力引发的隐私保护风险等。IPv6 与 5G 的融合应用，也将放大各类 5G 安全风险，应根据 5G 安全风险类型，重点强化网络、数据、设备等层面安全能力。

[36] IPv4 环境，DNS 仅需存储公有地址。
[37] IPv6 环境下，原有对全球 IPv4 地址进行全量扫描的方法已经失效，攻击者主要通过攻击递归 DNS 服务获取互联网资产情报，进而实施精准的地址扫描、网络攻击等。

- **物联网融合应用场景：**IPv6 与物联网融合场景下，海量物联网终端直接暴露在互联网下。部分物联网终端本身存在安全漏洞、非法接入等安全隐患，与 IPv6 的融合应用将导致现有物联网终端安全风险持续扩大。未来，应重点强化各类物联网终端安全防护能力，以及因终端安全隐患引发的各类安全问题的应对能力。

（三）构建 IPv6 安全创新机制，强化 IPv6 风险防范能力建设

一是推动建设联合创新中心，强化 IPv6 融合场景安全技术应对。联合产学研各界力量，推动成立 IPv6 安全联合创新中心，促进产学研用有机联动，深入挖掘 5G、物联网等新技术与 IPv6 融合场景下存在的未知安全风险，持续开展 IPv6 融合场景下安全风险应对技术研究，强化 IPv6 融合场景安全技术储备。**二是加快 IPv6 核心安全技术研究，构建下一代互联网安全体系架构。**根据 IPv6 升级改造情况，加快开展 IPv6 环境下编址语义、路由控制等基础资源管理核心技术研究，强化 IPv6 源地址管控、攻击溯源等网络安全手段探索研究，探索 IPv6 上网日志留存、数据报文解析等网络安全手段，进一步构建完善下一代互联网安全体系架构。**三是加快构建 IPv6 安全产品测试环境，强化 IPv6 安全产品孵化。**综合考虑 IPv6 安全产品发展现状，坚持“企业主体、多方合作”的工作原则，推动构建 IPv6 安全产品孵化平台和测试环境，加快在研 IPv6 安全产品孵化，优先孵化一批下一代互联网紧缺的 IPv6 安全产品的同时，验证当前 IPv6 安全产品应用性能。

（四）强化 IPv6 安全知识技能培训，弥合 IPv6 安全人才差距

一是加强 IPv6 安全知识和技能培训，提升 IPv6 相关工作人员安全能力。依托安全大会、安全培训等方式，重点面向政府、高校、中央企业、中央媒体等 IPv6 相关工作人员，加快开展 IPv6 网络安全教育和培训，助力 IPv6 环境下安全能力提升。**二是开展 IPv6 网络安全攻防竞赛，强化 IPv6 网络安全人员实战能力。**根据 IPv6 业务发展情况，鼓励相关科研机构搭建 IPv6 实际业务运行环境，开展 IPv6 环境下重点行业和领域网络安全攻防竞赛，提升网络安全人员实战能力。**三是强化 IPv6 网络安全专业人才培养，满足新环境下人才需求。**建立健全多层次人才培养，着力加强 IPv6 网络安全研究、管理、服务、工程等环节安全专业人才培养，弥补 IPv6 新业务、新场景下网络安全专业人才缺口。

中国信息通信研究院

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62304839、62300128

传真：010-62304980

网址：www.caict.ac.cn